Notes:
1. Untranslatable words are replaced with asterisks (****).
2. Texts in the figures are not translated and shown as it is.

Translated: 04:36:29 JST 07/21/2007
Dictionary: Last updated 07/20/2007 / Priority: 1. Information communication technology (ICT) / 2. Electronic engineering / 3. JIS (Japan Industrial Standards) term

FULL CONTENTS

[Claim(s)]
[Claim 1] The cryptographic key change method for authentication which a random number is used as the cryptographic key for authentication, compares the existing cryptographic key for authentication with the newly generated random number, and is characterized by using the random number as the new cryptographic key for authentication in card authentication data generation equipment when the comparison is inharmonious.
[Claim 2] The cryptographic key change method for authentication characterized by newly using as the cryptographic key for authentication the value which performed the operation which changes with fixed laws each time to initial value in card authentication data generation equipment, and this acquired.
[Claim 3] The cryptographic key change method for authentication characterized by performing the operation which changes with fixed laws each time to initial value in card authentication data generation equipment, enciphering the value which this acquired by the predetermined encryption method, and considering it as the new cryptographic key for authentication.
[Claim 4] The cryptographic key generation means for authentication is prepared in card authentication data generation equipment and card authentication center equipment. Make the above-mentioned cryptographic key generation means for both authentications hold the same initial value, and the above-mentioned card authentication data generation equipment receives the initial value. Perform the operation which changes with fixed laws each time, use the value as the cryptographic key for authentication, and [the above-mentioned card authentication center equipment] The cryptographic key change method for authentication characterized by carrying out to the operation which changes each time with said fixed law that the result of an operation does not agree with said cryptographic key for authentication, and different fixed laws to the initial value, and using the value as the cryptographic key for authentication.
[Claim 5] The cryptographic key generation means for authentication is prepared in card authentication data generation equipment and card authentication center equipment. Make the cryptographic key generation means for both [these] authentications hold the same initial value, and the above-mentioned card authentication data generation equipment receives the initial value. Perform the operation which changes with fixed laws each time, use as the new cryptographic key for authentication the value which enciphered to the value which this acquired, and [the above-mentioned card authentication center equipment] The cryptographic key change method for authentication characterized by using as the new cryptographic key for authentication the value which enciphered to the value which performed the operation which changes each time with different fixed laws which do not agree with the value acquired according to the operation of the above-mentioned card authentication data generation equipment to the initial value, and acquired it by this.
[Claim 6] [two or more keys generated by which new key generating method for authentication of Claims 1-5] If there is an authentication demand of the subsequent beginning for every card whenever it prepares for card authentication center equipment for every card and gives updating directions to card authentication center equipment The secure data of the card is enciphered using other one of the cryptographic keys for authentication prepared for the card one by one. The cryptographic key change method for authentication given in any of the Claims 1-5 characterized by writing the encryption data in a card with the above-mentioned authentication demand as secret information for authentication, and changing the cryptographic key for authentication they are.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Although there is a system which attests the data recorded on Information Storage Division media, such as an IC card, by encoding technology, and provides various services In the authenticating processing in such a system, this invention relates to the method of updating the cryptographic key currently used for authenticating processing to a different new cryptographic key for authentication from this, in order to raise the intensity to a code attack.

[0002]

[Description of the Prior Art] The terminal which possesses a public-key-encryption processing facility in the former, and the method of updating secret information by the side of the IC card on condition of user equipment, such as an IC card, are proposed by JP,H6-150082,A.

[0003]

[Problem to be solved by the invention] Since it becomes the public-key-encryption processing method has large processing load as compared with the secret key cipher processing method, and great [the method / the amount of data of a cryptographic key or secret information], it is not suitable for the service system which needs to offer a terminal and an IC card inexpensive. On the other hand, the secret key cipher processing method needs to deliver the same cryptographic key as the key used at the time of encryption to the equipment to decode, and the danger of disclosure is in it at the time of delivery.

[0004] As a method of avoiding such danger, it is the method of holding only the enciphered secret information, sending the secret information to card authentication center equipment through a terminal at the time of use, decrypting in card authentication center equipment, and verifying in an IC card. That is, card authentication center equipment holds the cryptographic key information for every card, and decodes and verifies it with the cryptographic key. Thus, the danger of cryptographic key disclosure can be suppressed.

[0005] When it is revealed according to injustice etc. as the cryptographic key by the side of card authentication center equipment is fixation, it becomes impossible however, to trust a card data authentication result. Offering the cryptographic key change method for authentication which changes the cryptographic key for authentication by the side of card authentication center equipment to a safe thing has this invention in order to solve this problem.

[0006]

[Means for solving problem] According to the 1st invention, in card authentication data generation equipment, a random number is used as the cryptographic key for authentication, the existing cryptographic key for authentication is compared with the newly generated random number, and when the comparison is inharmonious, let the random number be a new cryptographic key for authentication.

[0007] According to the 2nd invention, let the value generated by the fixed law be a new cryptographic key for authentication to initial value in card authentication data generation equipment. For example, let the key generated by the x-th be the value which counted up only x from initial value. In this example, it is considered as the value adding a value different each time to initial value. According to the 3rd invention, in card authentication data generation equipment, the value which changes with fixed laws each time is generated to initial value, the generated value is enciphered by the predetermined encryption method, and it is considered as the new cryptographic key for authentication.

[0008] According to the 4th invention, the cryptographic key generation means for authentication Card authentication data generation equipment, Prepare in card authentication center equipment and the above-mentioned cryptographic key generation means for both authentications is made to hold the same initial value. The above-mentioned card authentication data generation equipment performs the operation which changes with fixed laws each time to the initial value, uses the value as the cryptographic key for authentication, and [the above-mentioned card authentication center equipment] It carries out to the operation which changes each time with said fixed law that the result of an operation does not agree with said cryptographic key for authentication, and different fixed laws to the initial value, and let the value be a cryptographic key for authentication.

[0009] For example, use as the cryptographic key for authentication the value which added only 2x-1 to initial value the x-th with card authentication data generation equipment, and let the value which added 2x to initial value be a new cryptographic key for authentication at card authentication center equipment. According to the 5th invention, the cryptographic key generation means for authentication Card authentication data generation equipment, Prepare in card authentication center equipment and [the cryptographic key generation means for both / these / authentications] Make the same initial value hold and the above-mentioned card authentication data generation equipment receives the initial value. Perform the operation which changes with fixed laws each time, use as the new cryptographic key for authentication the value which enciphered to the value which this acquired, and [the above-mentioned card authentication center equipment] The operation which changes each time with different fixed laws which do not agree with the value acquired according to the operation of the above-mentioned card authentication data generation equipment is performed to the initial value, and let the value which enciphered to the value which this acquired be a new cryptographic key for authentication.

[0010] [two or more keys generated in the 6th invention by the above 1st or which / 5th / new key generating method for authentication] If there is an authentication demand of the subsequent beginning for every card whenever it prepares for card authentication center equipment for every card and gives updating directions to card authentication center equipment Using other one of the cryptographic keys for authentication prepared for the card one by one, the secure data of the card is enciphered, it writes in the card which had the above-mentioned authentication demand in the encryption data as secret information for authentication, and the cryptographic key for authentication is changed into it.

[0011]

[Mode for carrying out the invention] The method of this invention is applicable to drawing 1 . The example of functional constitution of a system is shown. It is an IC card and, as for the card 10, the secret information EK for authentication (S) as which the card identity information ID and a card 10 enciphered the generation number G and certification data (secure data) S which identify the cryptographic key for authentication used now with the cryptographic key K is held in the card 10.

[0012] The terminal 20 could detach and attach the card 10 and is equipped with the reader writer 21 which can write in the information which read the information, card authentication center equipment 30 and a data transmitting means 22 to receive [which receive and transmit data], and the data receiving means 23, to the attached card 11. A data receiving means 31 by which card authentication center equipment 30 receives the data from a terminal 20, Two cryptographic keys K for authentication for every card ID, K', and the storage section 32 Flag F and the secure data (data for authentication) S are remembered to be, respectively, [the storage section 32 / card / ID / which was received with an ID search means 33 to search with Card ID, and the data receiving means 31] A decoding means 34 to take out the cryptographic key K, K', Flag F, and the secure data S, and to decode the secret information EK (S) by K or K' according to G which received, A secure data verification means 35 to verify as compared with the decoded secure data S and S of the ID taken out from the storage section 32, A generation number verification means 36 by which the value of the generation number G in the data received with the data receiving means 31 performs that verification which is what kind of thing, A generation number change means 37 to perform processing which changes the generation number G if it will be necessary to change the generation number G which should be held on a card 10, a flag change means 38 to change the flag F of the storage section 32 if flag changing instruction is inputted, and when the cryptographic key for authentication is changed It has an encryption means 39 to encipher the secure data 5 of Correspondence ID with the new key K (K'), and to transmit to a terminal 20.

[0013] The reader writer 41 which writes in data or takes out data to the card 10 which card authentication data generation equipment (usually card issuing machine) 40 could detach and attach the card 10, and was attached, A key generation means 42 to generate the key K for authentication (K'), and a secure data generation means 43 to generate the secure data S, A card ID generation means 44 to generate Card ID, and an encryption means 45 to encipher the generated secure data 5 with the generated cryptographic key K for authentication (K'), It has a means 46 to generate the generation number G, a means 47 to generate Flag F, and a data transmitting means 48 to transmit the generated cryptographic key K for authentication (K'), the secure data S, Card ID, and Flag F to card authentication center equipment 30. Card ID, encryption secure data, EK (S) or EK' (S), and the generation number G are written in a card 10 by a reader writer 41.

[0014] the updating directions terminal 50 is equipped with the updating directions means 51, and every cycle which the operator decided suitably or beforehand, and the state where it decided beforehand occur -- ** -- alike -- etc. -- updating directions are generated suitably and it inputs into card authentication center equipment 30. If updating directions are inputted into card authentication center equipment 30 from the updating directions terminal 50 as shown in drawing 2 (S1), card authentication center equipment 30 will make "1" all the flags F in the storage section 32 (S2).

[0015] Then, ID of a card 10, G if EK (S) is sent to card authentication center equipment 30 through a terminal 20 the -- ID -- storage -- the section -- 32 -- searching -- corresponding -- K -- K -- ' -- F -- S -- reading (S3) -- moreover -- the generation number -- verification -- a means -- 36 -- having received -- G -- ″ -- zero -- ″ -- or -- investigating (S4) -- ″ -- zero -- ″ -- it is -- if -- [decode EK (S) which received by read K (S5), and] if G which received is not ″0″ [decode EK (S) which received using read K' (S6), investigate whether it is in agreement with S which which this decoded result read (S7), and] if [verification considers it as a failure, when in agreement, mean passing verification, read F investigates whether it is ″0″ (S8), and] if it is ″0″ S is enciphered with Key K in the same cryptographic key as the cryptographic key of the encryption means 45 of the issue machine 40, and the cryptographic key used for decode, and this case, and that EK (S), and ID and G are sent to a card 10 through a terminal 20 (S9).

[0016] The cryptographic key used for the cryptographic key of the encryption means 45, and decode when F was not ″0″, and a different cryptographic key, In this case, S is enciphered by key K' (S10), and if it is change, i.e., ″1″, with the generation number verification means 37 about G further, if it is ″0″, after changing into ″1″ (S11), that FK' (S), and ID and G are sent to ″0″ through a terminal 20 to a card 10. Then, F in the storage section 32 of the ID is made into ″0″ (S12).

[0017] Next, the card issuing processing at the time of using the method of the 1st invention with reference to drawing 3 is explained. In card authentication data generation equipment (it is described as an issue machine below) 40, Card ID is generated with the card ID generation means 44 (S1). A random number R is generated with the random number generation means 421 of the key generation means 42 (S2).

[0018] The random number R, key in the storage section 422, and comparing element 423 are compared, and it is investigated whether there is any match (S3). When not in agreement, it investigates whether the inequality is the 1st time (S4), and if it is the 1st time, the R will be written in as a key K and it will register with the storage section 422 with a means 424 (S5). When in agreement at Step S3, R is discarded, it returns to Step S2, and a random number is generated again.

[0019] When the writing of the storage section 422 is 1 time that is, at Step S4, it returns to Step S2, comparison with generating of a random number R and the key in the storage section 422 is repeated, and when not in agreement, it writes in the storage section 422 as key K' (S6). The secure data generation means 43 generates the secure data S (S7). S is enciphered with the encryption means 45 using Key K, and EK (S) is generated (S8).

[0020] It is considered as a flag F= 0 with the flag generation means 47, and is considered as the generation number G= 0 with the key generation means 46 (S9). The issue machine 40 transmits Cards ID and K, K', F, and S to card authentication center equipment 30. Moreover, the issue machine 40 stores Cards ID and G and EK (S) in a card 10.

[0021] Next, the card issuing processing in the case of using the method of the 2nd invention is explained with reference to drawing 4 . The issue machine 40 generates Card ID (S1). The key value KV of a register 425 is advanced with the operation means 426 by the key generation means 42. that is, the value set to KV+1=K (it carries down, that is, 2 is KV-1=K) is used as Key K, further, with the write-in means 424, by setting K to KV, it writes in and advances to a register 425 (or moving down), and ** is made into key K'. Moreover, newly let key K' at this time be a key value KV (S2).

[0022] An issue machine generates the secure data S (S3). With an issue machine, S is enciphered using the encryption means 45 and Key K, and EK (S) is generated (S4). It is considered as a flag F= 0 and the generation number G= 0 like the 1st invention (S5). The issue machine 40 transmits Cards ID and K, K', F, and S to card authentication center equipment 30.

[0023] The issue machine 40 stores Cards ID and G and EK (S) in a card 10. Next, the case where card issuing processing is performed using the method of the 3rd invention is explained with reference to drawing 5 . The issue machine 40 generates Card ID (S1). Let the value which advanced the key value KV of the register 425 with the operation means 426 (or moving down), and enciphered the ** value with the cryptographic key HK for issue equipment with the encryption means 45 be Key K with the key generation means 42. What advanced the key value KV further similarly (moving down), and enciphered the ** value is made into key K'. Moreover, it newly writes in a register 425 by making the value at this time (initial value of key K') into a key value KV (S2). In addition, the cryptographic key generation means 427 for issue equipment generates Key HK.

[0024] An issue machine generates the secure data S like a front case after that (S3). With an issue machine, S is enciphered with the encryption means 45 using Key K, and EK (S) is generated (S4). It is considered as a flag F= 0 and the generation number G= 0 (S5). An issue machine transmits Cards ID and K, K', F, and S to card authentication center equipment 30.

[0025] An issue machine stores Cards ID and G and EK (S) in a card 10. The case where card issuing processing is performed using the method of the 4th invention is explained with reference to drawing 6 . In this case, in advance, it is the issue machine 40 and card authentication center equipment 30, a key value KV is shared, and as a solid line shows in card authentication center equipment 40' in drawing 1 , key generation means 32' is prepared.

[0026] An issue machine generates Card ID (S1). The key value KV of a register 425 is advanced 2x-1 with the operation means 426 by the key generation means 42 of an issue machine (or moving down), and let a ** value be Key K. Moreover, it newly stores in a register 425 by the write-in means 424 by making the key K at this time into a key value KV (S2).

[0027] The issue machine 40 generates the secure data S (S3). With the issue machine 40, S is enciphered using the encryption means 452 and Key K, and EK (S) is generated (S4). It is considered as a flag F= 0 and the generation number G= 0 (S5). The issue machine 40 transmits Cards ID and K, F, and S to card authentication center equipment 30.

[0028] Card authentication center equipment 30 itself 2x Advances the key value KV of register 425' with the operation means 426 by key generation means 32' (or moving down), and it makes a ** value key K'. Moreover, it newly stores in register 425' by write-in means 474' by making key K' at this time into a key value KV (S6). The issue machine 40 stores Cards ID and G and EK (S) in a card 10.

[0029] Furthermore, the card issuing processing using the method of the 5th invention is explained with reference to drawing 7 and drawing 8 . Also in this case, in advance, the issue machine 40 and card authentication center equipment 30 share a key value KV, and key generation means 32' is prepared in card authentication center equipment 30 with them. An issue machine generates Card ID (S1). Let the value which advanced the key value KV in a register 425 2x-1 with the operation means 426 by the key generation means 42 of the issue machine (or moving down), and enciphered the ** value with the enciphering key HK for issue equipment with the encryption means 45 be Key K. Moreover, a key value KV is advanced 2x-1 (moving down), and it newly writes in a register 425 by making a ** value into a key value KV, and stores with a means 424 (S2).

[0030] An issue machine generates the secure data S (S3). With an issue machine, S is enciphered with the encryption means 42 using Key K, and EK (S) is generated (S4). It is considered as a flag F= 0 and the generation number G= 0 (S5). The issue machine 40 transmits Cards ID and K, F, and S to card authentication center equipment 30.

[0031] With the reception generation means 42 of card authentication center equipment 40, the value which 2x Advanced the key value KV of register 423' (or moving down), and enciphered the ** value with encryption means 45' and the enciphering key HK for issue equipment is made into key K'. Moreover, the key value KV at this time is 2x Advanced (moving down), and it newly writes in register 425' by making a ** value into a key value KV, and stores by means 424' (S6).

[0032] An issue machine stores Cards ID and G and EK (S) in a card. Whenever it advanced the key value in drawing 6 (moving down), the result of an operation K was made into initial value KV, but the initial value set up first may be used as it is, that is, the operation of KV=K and KV=K' may be omitted. You may use KV set up first each time, without updating initial value by KV=KV+ (2x-1) and KV=KV+2x in drawing 7 . Moreover, in ****, what the personal computer and the PC card combined is [that the card 10 should just be what memory and communication facility occur and can perform read-out and writing by a reader writer to the memory that is,] sufficient not only as an IC card but an example.

[0033]

[Effect of the Invention] As stated above, according to this invention, the unique nature of a key is guaranteed, that is, since it changes into the existing cryptographic key and a conflicting cryptographic key, the cryptographic key attack which may have been generated by then can be repealed. Renewal of all the keys that the database (storage section 32) of card authentication center equipment permits is possible. That is, what is necessary is to prepare further many keys and just to repeat using these one by one for every updating directions, although two keys K and K' were used by turns about each card in the above-mentioned example.

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the example of functional constitution of the system by which this invention method is applied.

[Drawing 2] The flow chart showing the example of the procedure in the card authentication center equipment 30 in drawing 1 .

[Drawing 3] The flow chart showing the example of the card issuing procedure with which A used the method of the 1st invention, and B are the block diagrams showing the functional constitution of the cryptographic key generation means for authentication.

[Drawing 4] The flow chart showing the example of the card issuing means for which A used the method of the 2nd invention, and B are the block diagrams showing the functional constitution of the cryptographic key generation means for authentication.

[Drawing 5] The flow chart showing the example of the card issuing procedure with which A used the method of the 3rd invention, and B are the block diagrams showing the functional constitution of the cryptographic key generation means for authentication.

[Drawing 6] The flow chart showing the card issuing procedure and the key generation procedure of card authentication center equipment which A used the method of the 4th invention, and B are the block diagrams showing the functional constitution of the cryptographic key generation means for authentication.

[Drawing 7] The flow chart showing the card issuing procedure using the method of the 5th invention, and the key generation procedure of card authentication center equipment.

[Drawing 8] The block diagram showing the functional constitution of the cryptographic key generation means for authentication.

[Drawing 8]

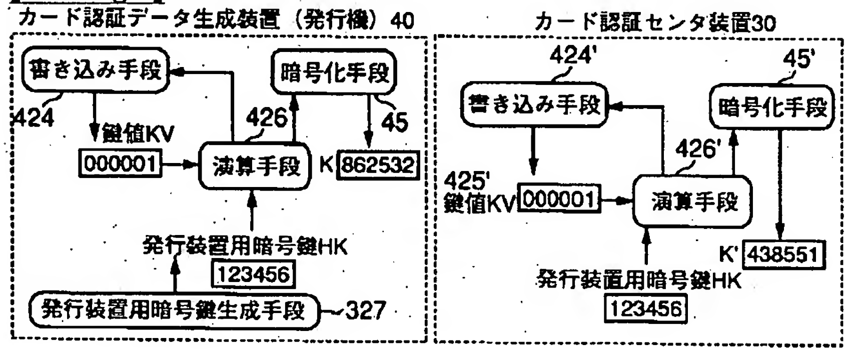

図8

[Drawing 1]

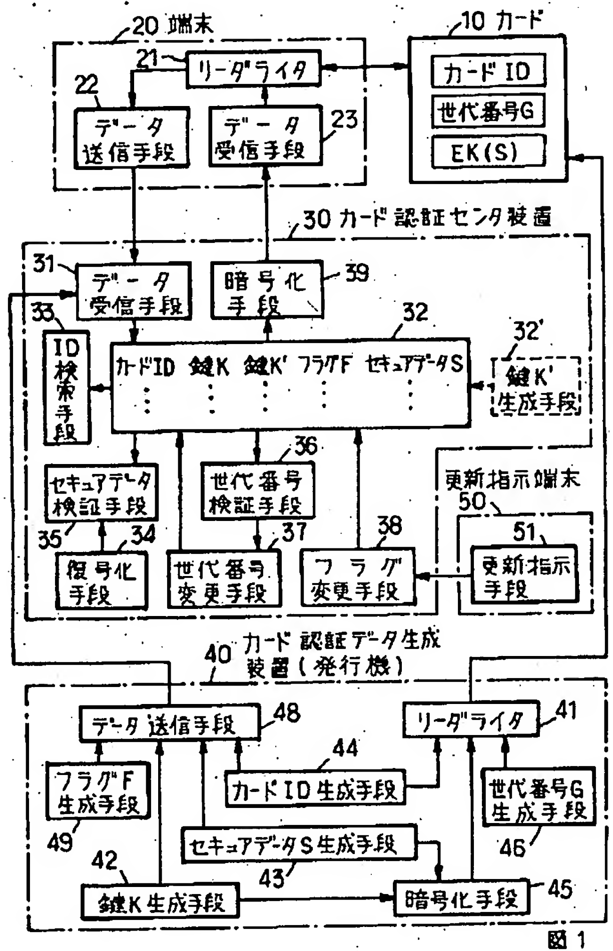
20 端末
10 カード
21
リーダライタ
22
データ送信手段
データ受信手段
23
カードID
世代番号G
EK(S)
30 カード認証センタ装置
31
データ受信手段
暗号化手段
39
33
ID検索手段
32
カードID
鍵K
鍵K'
フラグF
セキュアデータS
32'
鍵K'生成手段
36
セキュアデータ検証手段
世代番号検証手段
更新指示端末
50
35
34
37
38
51
更新指示手段
復号化手段
世代番号変更手段
フラグ変更手段
40 カード認証データ生成装置(発行機)
データ送信手段
48
リーダライタ
41
44
カードID生成手段
フラグF生成手段
49
世代番号G生成手段
46
セキュアデータS生成手段
43
42
鍵K生成手段
暗号化手段
45

図 1

[Drawing 2]

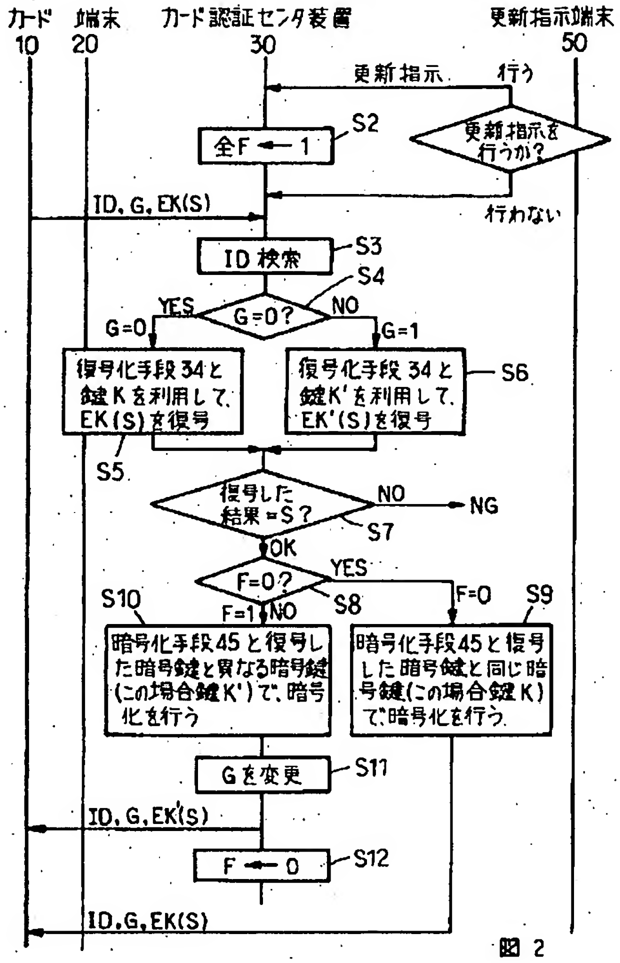

図 2

[Drawing 7]

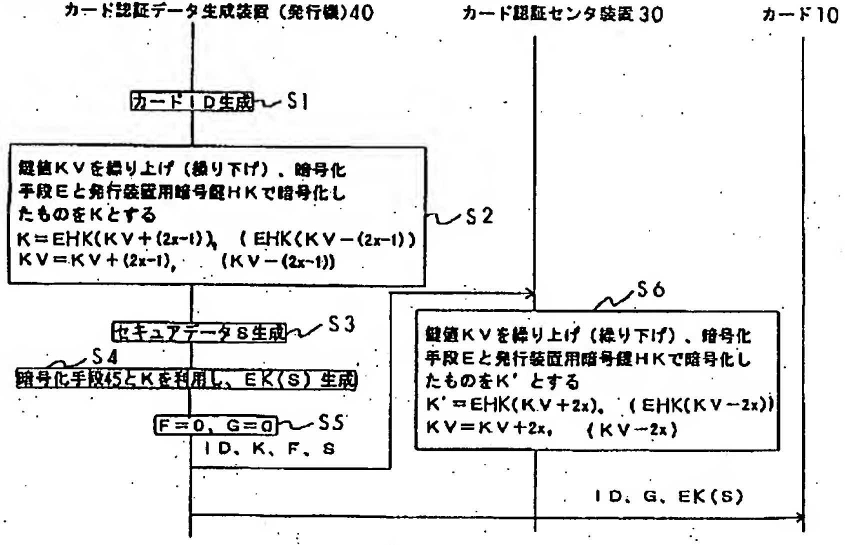
カード認証データ生成装置（発行機）40
カード認証センタ装置30
カード10
カードＩＤ生成
S1
鍵値ＫＶを繰り上げ（繰り下げ）、暗号化手段Ｅと発行装置用暗号鍵ＨＫで暗号化したものをＫとする
K＝EHK(ＫＶ＋(2x−1))，（EHK(ＫＶ−(2x−1))
ＫＶ＝ＫＶ＋(2x−1)，（ＫＶ−(2x−1))
S2
セキュアデータＳ生成
S3
S4
暗号化手段45とＫを利用し、ＥＫ(Ｓ)生成
F＝0，G＝0
S5
ＩＤ、Ｋ、Ｆ、Ｓ
S6
鍵値ＫＶを繰り上げ（繰り下げ）、暗号化手段Ｅと発行装置用暗号鍵ＨＫで暗号化したものをＫ' とする
K'＝EHK(ＫＶ＋2x)，（EHK(ＫＶ−2x))
ＫＶ＝ＫＶ＋2x，（ＫＶ−2x）
ＩＤ、Ｇ、ＥＫ(Ｓ)

図 7

[Drawing 3]

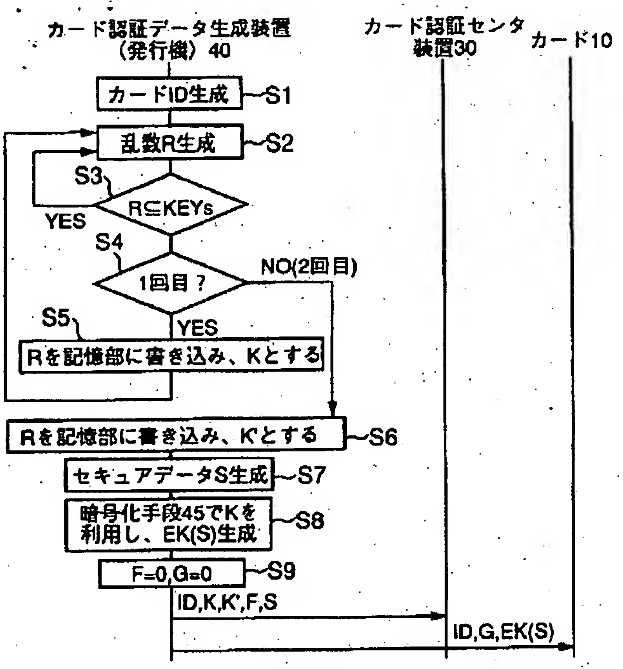

図3A

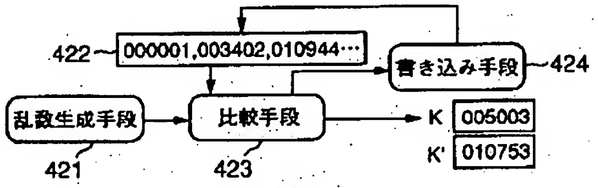

図3B

[Drawing 4]

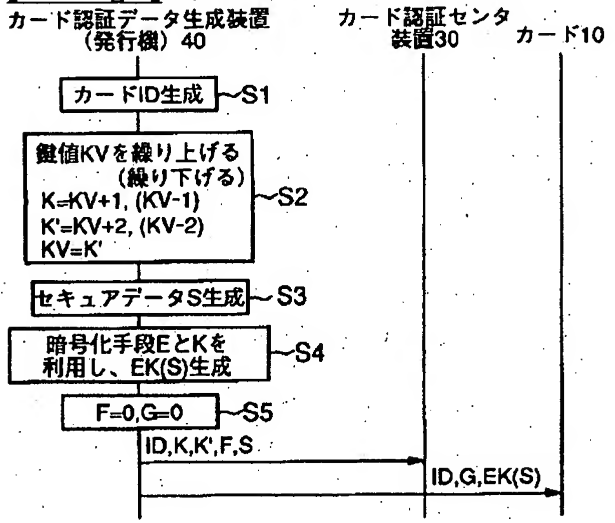

図4A

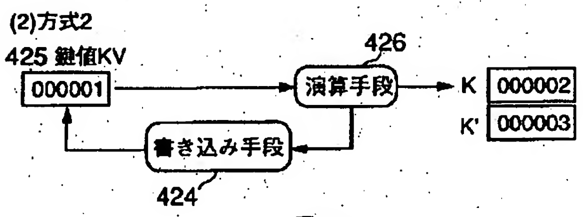

図4B

[Drawing 5]

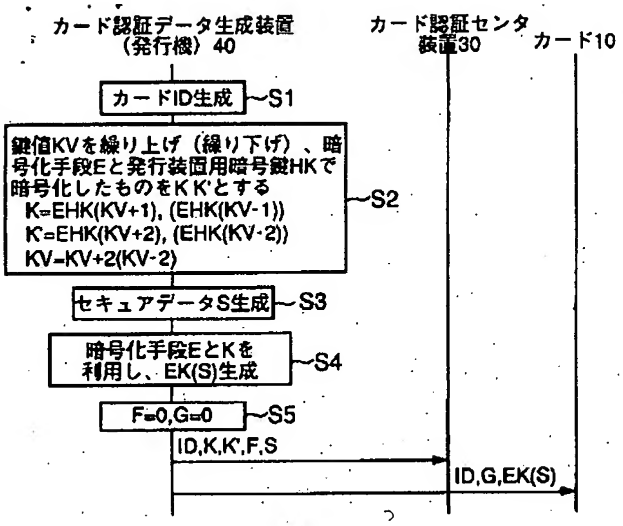

図5A

(3)方式3

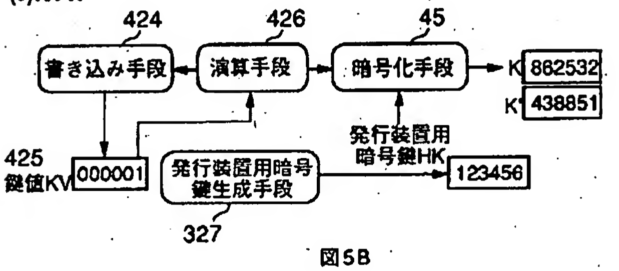

図5B

[Drawing 6]

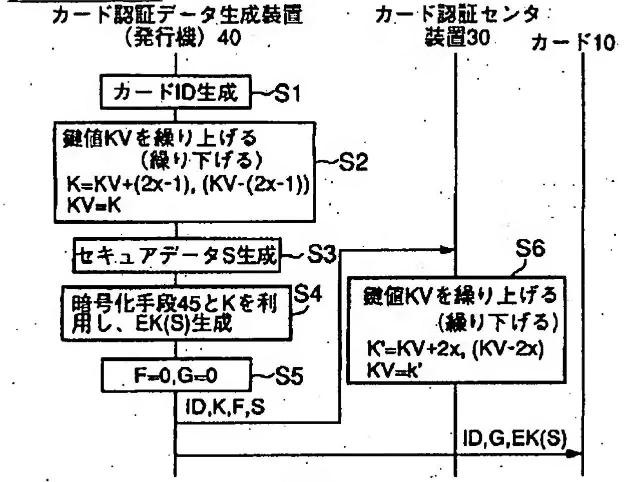

図6A

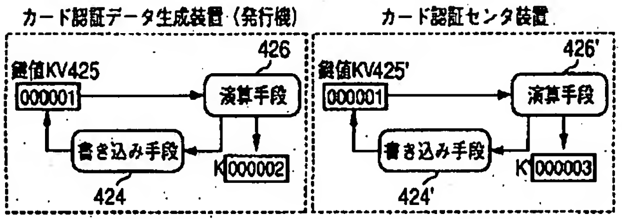

図6B

[Translation done.]